IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH CELL PHONE ACCOUNTS (540) 206-7320 AND (540) 519-4047 THAT ARE STORED AT PREMISES CONROLLED BY T-MOBILE WIRELESS PROVIDER	Case No. 7:24mj92 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Brian P. McBride, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by T-Mobile, a wireless provider headquartered at 4 Sylvan Way, Parsippany, New Jersey. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require T-Mobile to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Task Force Officer with the Bureau of Alcohol, Tobacco, Firearms and Explosives, and have been since approximately April, 2021. I am employed by the Roanoke County Police Department as a detective and have been a sworn law enforcement officer within the Commonwealth of Virginia for approximately ten years. During that time, I have conducted several hundred narcotics investigations and have received specialized law enforcement training on a variety of related matters.

3. During my career, I have participated in the execution of numerous arrest and search warrants for criminal offenses involving the possession with the intent to distribute controlled substances and the distribution of controlled substances. I am familiar with the methods drug traffickers use to conduct their illegal activities, to include communication methods, vehicle usage, text messaging, and narcotics transactions.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, probable cause exists to believe that David Leon Abrams ("ABRAMS"), Shaquan Lacole Webb ("WEBB"), and other unknown individuals committed violations of 21 U.S.C. §§ 841(a)(1) and 846 in the Western District of Virginia. Probable cause also exists to search the information described in Attachment A for evidence of these crimes

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. On May 29, 2024, an ATF-Roanoke confidential informant (hereinafter "CI") met with ABRAMS to conduct a controlled purchase of what ABRAMS described as being black tar heroin. The CI arranged this purchase with ABRAMS by texting and calling ABRAMS at the

number (540) 206-7320 ("SUBJECT PHONE 1"). The CI's call and texts with ABRAMS were recorded. Law enforcement verified that T-Mobile provides service to SUBJECT PHONE 1 and that this number is used by ABRAMS.

8. The CI is a convicted felon with convictions for larceny and drug related crimes, however, the CI has provided extensive amounts of information to law enforcement that has been deemed accurate through audio/video recordings, surveillance, and other means of investigation.

9. During the May 29, 2024, controlled purchase, law enforcement met the CI at a predetermined location and searched both their person and vehicle. Law enforcement provided the CI $500 in pre-recorded official government funds and maintained surveillance while the CI drove to ABRAMS' house. At approximately 3:15 p.m., ABRAMS invited the CI inside his residence located at 2516 Oakland Blvd NW, Roanoke, Virginia. While inside, ABRAMS received a phone call from an unknown individual believed to be ABRAMS' supplier. ABRAMS then requested that the CI provide him with the money so that he could meet his supplier outside. Accordingly, the CI provided ABRAMS with $460 of official government funds.

10. At approximately 3:43 p.m., law enforcement observed a white Nissan Altima with 30-day temporary Virginia registration 74296F arrive in the driveway of ABRAMS' residence. The vehicle was registered to WEBB, who is believed to be ABRAMS' relative. Surveillance units observed two individuals in the Nissan but did not get a positive identification on either one. Law enforcement then observed ABRAMS come outside the residence and meet with the occupants of the vehicle before returning inside. Once back inside, ABRAMS provided the CI with approximately 8 grams of suspected heroin.

11. Using a subpoena, law enforcement later learned that SUBJECT PHONE 1 communicated with phone number (540) 519-4047 ("SUBJECT PHONE 2") throughout May 29, 2024. The subject phones communicated with each other at 3:07 p.m., 3:13 p.m., 3:39 p.m., and 3:40 p.m., which times corresponded to the Nissan arriving to 2516 Oakland Blvd NW. Law enforcement determined that SUBJECT PHONE 2 is provided service through T-Mobile and is subscribed to WEBB.

12. On June 5, 2024, at approximately 2:06 p.m., the CI conducted a second controlled purchase of 29.3 grams of suspected fentanyl from ABRAMS from within 2516 Oakland Blvd NW. As with the previous occasion, the CI arranged the transaction by text and phone call with ABRAMS by contacting SUBJECT PHONE 1. Prior to the deal, law enforcement met the CI at a predetermined location and searched both their person and vehicle. Law enforcement provided the CI $1600 in pre-recorded official government funds and maintained surveillance while the CI drove to ABRAMS house. The CI exchanged the $1600 with ABRAMS for the suspected fentanyl.

13. On June 18, 2024, the CI and ABRAMS engaged in a text communication using the SUBJECT PHONE 1 number. During the conversation, ABRAMS stated his nephew was a kilogram level supplier of narcotics. The conversation included prices and ABRAMS indicated that the CI would have to purchase 5 zips to get a better price. Based on my training, experience, and the context of the conversation, I know zips to be a common slang term for an ounce of narcotics.

14. On June 26, 2024, the CI conducted a third controlled purchase of 59.6 grams of suspected fentanyl from ABRAMS from within 2516 Oakland Blvd NW. Law enforcement implemented controls by meeting the CI at a predetermined location and searching both thier

person and vehicle, providing them with pre-recorded official government funds, and maintaining surveillance.

15. At approximately 11:54 a.m., June 26, 2024, the CI arrived at ABRAMS' residence at 2516 Oakland Blvd NW. The CI arranged this transaction with ABRAMS by communicating with ABRAMS at SUBJECT PHONE 1. While the CI was in the residence with ABRAMS, surveillance units observed WEBB leave 4227 Hershberger Rd NW[1] and drive directly to 2516 Oakland Blvd NW. Surveillance units then saw ABRAMS walk over and meet with the driver of the Nissan for less than a minute and then walk back towards 2516 Oakland Blvd NW. Once back inside, ABRAMS provided the CI with the suspected fentanyl in exchange for $3000. The substance the CI purchased later field tested positive for fentanyl utilizing a Premier Bio-Dip test kit.

16. Based on subpoena returns, law enforcement has established that between May 24, 2024, and June 26, 2024, SUBJECT PHONE 1 and SUBJECT PHONE 2 communicated with each other over 150 times, including approximately 80 text messages. Based on my training and experience, individuals engaged in criminal drug conspiracies involving activities such as distribution frequently use cell phones and text messages to communicate and coordinate orders, deliveries, prices, and locations. On June 27, 2024, a preservation request was sent to T-Mobile for data under the accounts of SUBJECT PHONE 1 and SUBJECT PHONE 2.

17. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public, and that stored electronic

[1] Investigators have linked WEBB to this address through a combination of law enforcement and open-source databases.

communications, including retrieved and unretrieved voicemail, text, and multimedia messages for T-Mobile subscribers may be located on the computers of T-Mobile. Further, I am aware that computers located at T-Mobile contain information and other stored electronic communications belonging to unrelated third parties.

18. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of T-Mobile for weeks or months.

19. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS") and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by T-Mobile for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

20. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations,

lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

21. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

22. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which "cell towers" (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

23. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

24. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

25. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a

wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such "timeline" information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device's owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require T-Mobile to disclose to the government copies of the records and other information

(including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

27. Based on the forgoing, I submit that probable cause exists to believe that ABRAMS and WEBB used SUBJECT PHONE 1 and SUBJECT PHONE 2 to coordinate and facilitate illegal drug transactions. Further, I submit that probable cause exists to believe that the information requested from T-Mobile will likely contain evidence of the crimes under investigation and will assist law enforcement in identifying suspected individuals yet unknown. As such, I respectfully request that the Court issue the proposed search warrant.

REQUEST FOR SEALING

28. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Brian P. McBride
Task Force Officer

ATF

Subscribed and sworn to before me on July 12, 2024 by telephone.

UNITED STATES MAGISTRATE JUDGE